REMARKS

Claims 1-24 are pending in this application. Claims 1 and 24 have been amended. Applicants respectfully request reconsideration and allowance of the claims based on the claims amendment and the following remarks.

REJECTIONS UNDER 35 U.S.C. §102(b)

Claims 1-24 are rejected under §102(b) as being anticipated by Rezaiifar et al. (USP 6,980,658). Applicants traverse this rejection.

Without acquiescing to the Examiner's allegations, Applicants have amended independent claims 1 and 24 for clarification purposes.

Independent claims 1 and 24 recite similar features, accordingly, for brevity the patentability of the claims will be discussed with respect to claim 1. The Examiner alleges that Rezaiifar et al. teaches deriving two (2) cryptosync values. For support, the Examiner specifically cites column 2, lines 25-38.

Column 2, lines 25-38 of Rezaiifar et al. provides:

> In one aspect, a method for transmitting authentication variables from a transmission end to a receiving end is presented, the method comprising: generating a crypto-sync value at the transmission end; generating a first authentication signature from the crypto-sync value and an encryption key at the transmission end; transmitting the crypto-sync value and the first authentication signature to the receiving end; generating a second authentication signature from the crypto-sync value and the encryption key at the receiving end; incrementing the crypto-sync value at the receiving end if the first authentication signature and the second authentication signature match; and requesting an encryption key exchange if the first authentication signature and the second authentication signature do not match. (Emphasis added.)

As can be seen from the quoted passage above, Rezaiifar et al. teaches that only a single crypto-sync value is generated. In the quoted passage above, Rezaiifar et al. teaches that two (2) authentication signatures are generated from a single crypto-sync value, but nowhere does it teach "deriving a value of a first cryptosync for the communication session, the first cryptosync having a life limited to the communication session, based on a value of a second cryptosync" recited in claim 1. (Emphasis added.)

Claim 1 has been amended for clarification, for example, claim 1 recites, *inter alia*, "the first cryptosync having a life limited to the communication session" and "the second cryptosync having a life extending over multiple communication session." The Examiner in rejecting claim 1 also alleges that Rezaiifar et al. teaches that "cryptosync are time values and its value will vary depending on transmitted data." For support, the Examiner cites column 4, lines 46-62 of Rezaiifar et al.

Column 4, lines 46-62 of Rezaiifar et al. provides:

> ENC_SEQ generator 202 provides a sequence number that is used to construct a crypto-sync value. In one aspect of the embodiment, the four least significant bits of a sequence number are used to construct a crypto-sync value. A crypto-sync value is a variable that is inputted to an encryption algorithm along with an encryption key. The encryption algorithm generates a mask through which unencrypted data is encrypted. Crypto-syncs differ from encryption keys in that an encryption key is a semi-permanent shared secret while a crypto-sync value will vary with respect to the data units transmitted during the link in order to protect against a replay attack. In this embodiment, the crypto-sync value will vary due to a dependence upon either a generated sequence number, a system time, or any other designated identifier. It should be noted that one may alter the number of bits used for the crypto-sync value without changing the scope of the embodiment. (Emphasis added.)

As can be seem from the quoted passage, nowhere does Rezaiifar et al. teach a first cryptosync and a second cryptosync. In addition, the quoted passage teaches that the cryptosync's value (i.e., numbers) is variable, unlike the encryption key. To allege that Rezaiifar et al. teaches "cryptosync are time values and its value will vary depending on transmitted data," the Examiner is alleging a feature that is simply not taught or suggested in Rezaiifar et al.

For at least the reasons given above, Applicants submit that independent claims 1 and 24 are patentable over Rezaiifar et al. In addition, dependent claims 2-23 are also patentable for depending on an allowable base claim.

THE REMAINDER OF THE PAGE HAS BEEN LEFT BLANK INTENTIONALLY

CONCLUSION

In view of the above remarks and amendments, the Applicants respectfully submit that each of the rejections has been addressed and overcome, placing the present application in condition for allowance. A notice to that effect is respectfully requested. If the Examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to contact the undersigned.

Pursuant to 37 C.F.R. §§ 1.17 and 1.136(a), Applicant(s) hereby petition(s) for a one (1) month extension of time for filing a reply to the outstanding Office Action and submit the required $120.00 extension fee herewith.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Gary D. Yacura at the telephone number of the undersigned below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By ______ Reg No. 45,261

XW
Gary D. Yacura, Reg. No. 35,416
P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

GDY/LYP:psy